



April 18, 2011

Chairman Mary Bono Mack
Subcommittee on Commerce,
Manufacturing & Trade
House Committee on Energy & Commerce
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, D.C. 20515

Ranking Member G.K. Butterfield
Subcommittee on Commerce,
Manufacturing & Trade
House Committee on Energy & Commerce
U.S. House of Representatives
2322A Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Bono Mack and Ranking Member Butterfield:

I am writing on behalf of Epsilon Data Management LLC ("Epsilon") to respond to your recent inquiry regarding the March 30, 2011 security incident involving unauthorized access of Epsilon's e-mail services platform. The incident resulted in the theft of lists containing e-mail addresses and, in some cases, first and last names maintained by Epsilon on behalf of a small percentage of its customers.

Epsilon values strongly the trust its customers place in it and their expectation that Epsilon will secure their data. The company continually monitors and evaluates its systems in an attempt to ensure their integrity. For these reasons, Epsilon deeply regrets that the criminal activities of others have called into question this commitment. The company continues to investigate the incident thoroughly and is cooperating with law enforcement to try and apprehend those responsible. As data management services become more sophisticated, criminals likewise are enhancing their efforts to infiltrate even the most sophisticated systems. Companies like Epsilon must continue to work with law enforcement at the national and state levels to ensure strong protections for data management companies, our customers and, most importantly, the end consumers whose data is at issue.

We hope that the following information answers your questions. We remain available to provide further information.

Background

Epsilon, a subsidiary of Alliance Data Systems Corporation, is a leading provider of permission-based e-mail marketing services. The company's roots lie in the direct mail marketing industry, where for over 40 years Epsilon has provided valuable services to companies seeking to market to consumers directly through postal mail, for example, through catalog



AllianceData™

7500 Dallas Parkway
Suite 700
Plano, TX 75024
214-494-3000

Loyalty and Marketing
Services

www.epsilon.com

marketing. Today, in addition to those and other related services, Epsilon also provides its customers with an e-mail marketing platform that includes enabling management of consumer e-mail contact information and implementation of opt-out requests. Consumers opt-in to receive communications from companies/brands (Epsilon customers) for which they have an affinity, and those e-mail communications can be notifications, special incentives, rewards and educational information, among others. Epsilon provides the mechanism through which companies can help ensure that consumer e-mail lists are maintained and messages to them (and their subscription preferences) are managed in accordance with Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (the "CAN-SPAM Act"). The platform enables customers and Epsilon employees, acting on their behalf as account managers, to manage this data.

As a provider of data management services to some major consumer brands and financial institutions, Epsilon is committed to responsible information governance and recognizes the importance of keeping client data secure. To enhance security across its databases, Epsilon has implemented and maintains an information-security program conforming to data security standards set forth by the International Organization for Standardization (ISO). The ISO 27001¹ management standards that implement ISO 27002² controls, established a checks and balances system. This system requires information-security management which systematically assesses an organization's information-security risks, designs and implements comprehensive safeguards to control unacceptable risks, and maintains that program to ensure continued improvement and ongoing assessments. The goal of the ISO 27002 standard is to facilitate best practices for controlling information-security risks of the type to which companies like Epsilon might be subject. For example, one of the controls employed by Epsilon that is particularly relevant to this incident is that the company segregates its systems hosting e-mail applications from its systems hosting other database solutions. Combined, the ISO 27001 standard and 27002 controls provide a process for comprehensive information security that is detailed, rigorous, and adaptable to changing circumstances.³

It is important to note that ISO certification is a thorough and demanding process. Epsilon began the process to implement and obtain ISO certification of its information-security program in 2005 and completed its certification in 2006. The certification process took nearly a year and involved coordination with Alliance Data Systems' internal audit group and required validation from third-party auditors. Since 2006, Epsilon has maintained its ISO 27001 certification, undergoing yearly reviews that demand continual improvements to the company's information-security program. By obtaining and maintaining this certification, Epsilon has demonstrated its commitment to ensuring its information-security program provides reasonable and appropriate safeguards for client and consumer data.

¹ International Organization for Standardization, ISO/IEC 27001:2005, http://www.iso.org/iso/catalogue_detail?csnumber=42103.

² International Organization for Standardization, ISO/IEC 27002:2005, http://www.iso.org/iso/catalogue_detail?csnumber=50297

³ Ted Humphreys, *State-of-the-Art Information Security Management Systems with ISO/IEC 27001:2005*, ISO INSIDER, Jan.-Feb., 2006, available at http://www.iso.org/iso/info_security.pdf

Chronology

Like many other organizations, Epsilon's information-security program is designed to identify and respond to new attacks and threats. Here, Epsilon's security program identified unauthorized activity with respect to certain of the company's e-mail databases and invoked Epsilon's security incident-response program. This led to an immediate move to investigate and remediate the unauthorized entry and to put in place additional safeguards based on what the company has learned so far, as the following chronology illustrates.

On March 30th, an Epsilon employee reached out to the security hotline maintained by the company. The employee had detected unusual download activity which seemed suspicious. Epsilon responded immediately with an investigation into the incident. This effort revealed that the login credentials of the employee, an e-mail application administrator, had been compromised. As soon as Epsilon's investigators identified the compromised credentials, the security team disabled the credentials and began a forensic investigation of the relevant computer resources.

Among the immediate responses, the company undertook the following:

- Initiated additional virus scans of relevant systems.
- Revoked and re-issued Epsilon system-user credentials for admin-level users.
- Invested and committed additional resources to monitoring unusual or suspicious activity.
- Began a forensic investigation to identify root causes.

In addition to efforts to identify and contain the incident within the company, Epsilon also began promptly assisting its customers. These actions included:

- Contacting potentially affected customers and cooperating with them on an ongoing basis.
- Notifying law enforcement including the FBI and Secret Service to seek out their assistance.
- Communicating with its anti-virus support vendor to identify threat signatures and obtain additional support.

After the initial day, Epsilon continued to investigate the incident, cooperate with law enforcement, and monitor its systems.

On April 1st, the Secret Service began its investigation. Epsilon continued its investigation and engaged outside forensic consultants to assist. The following day, April 2nd, Epsilon met with its outside forensic consultants to review the evidence collected thus far and confirm that information was flowing to the Secret Service. Epsilon's outside forensic consultants also reviewed the company's containment measures implemented thus far and, as the investigation unfolds, will make recommendations regarding further measures.

To date, the investigation has confirmed preliminarily that only e-mail addresses and, in some cases first and last names have been affected, involving approximately two percent of the company's total client base. At this time the company has no evidence that any other services or information it maintains has been affected. The company is seeking information regarding whether or not there has been any increase in unsolicited commercial e-mail or fraudulent or deceptive e-mail, including "phishing" attacks. It also appears that the incident was isolated to Epsilon's e-mail services platform; other platforms, such as its hosted customer databases, were not affected, as they, again, are segregated from the e-mail services platform.

Public reports indicate that at least 50 of Epsilon customers were impacted; some of those customers chose to notify their customers of the incident, and in some cases those customers made public statements. Epsilon's relationships with its customers are confidential, and at their request, their identity was not disclosed publicly by Epsilon. For that reason, we are unable at this time to provide a complete list of the company's affected customers, as Epsilon is still reviewing its confidentiality and notice obligations with its customers.

Epsilon is also attempting to ascertain the total number of individual consumers affected. Determining this number, however, may be difficult for several reasons. First, because many consumers use multiple e-mail addresses and may appear on several or many of Epsilon's customers' lists, identifying the number of individually affected consumers with any precision may not be possible. Similarly, Epsilon cannot determine how many consumers may have been affected within a particular state because the information as maintained generally only included an e-mail address (or name in some cases). Epsilon has, however, provided public notice of the incident on its website via press releases on April 1st and April 6th, and has set up an incident-response center to answer questions from consumers and customers who contact the company. Epsilon has also added information to its website to provide educational materials for consumers on guarding against phishing attacks, available at [http://www.epsilon.com/Privacy%20Policy/Consumer Information on Phishing/p467-12](http://www.epsilon.com/Privacy%20Policy/Consumer%20Information%20on%20Phishing/p467-12). This website provides information to consumers explaining phishing attacks, how they occur, and the steps a consumer can take to avoid being a victim.

We hope that the information above responds to the questions you posed and provides context for the attack that occurred on Epsilon's e-mail services platform. In addition, with regard to your question concerning how personal data is retained, Epsilon maintains its customers' e-mail address lists per the guidance of its customers upon whose behalf we maintain this data. The duration of the retention of that data likewise is done at our customers' direction. Finally, in reply to your query regarding whether Epsilon plans to offer any credit monitoring or other services to consumers, at this time, Epsilon is still investigating the potential implications of this attack on individual consumers. The company has not made an evaluation of whether it would be appropriate to provide credit monitoring or other services to consumers.

Moving Forward

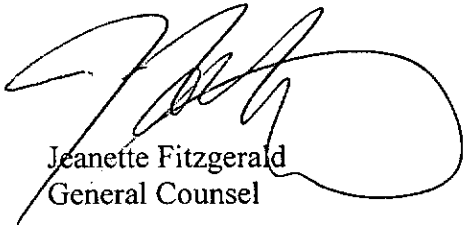
Going forward, Epsilon will continue to adhere to and improve its security policies and procedures, especially in light of this criminal attack on its e-mail services platform. Further, Epsilon has engaged third-party services to review and recommend additional hardening processes to the company's existing controls.

We should also note that it remains Epsilon's first priority to respond to its customers and ensure they have the company's full cooperation so that their data and consumers are protected. The company anticipates identifying additional facts as part of its existing practice to remediate incidents and learn from them. As this effort is completed, Epsilon remains committed to cooperating fully.

* * * * *

We sincerely hope that this information answers your questions regarding this malicious attack on Epsilon's systems. The company continues to make significant efforts to remediate this situation and to work to prevent such breaches from occurring again. Epsilon will also continue to fully cooperate with law enforcement to identify the perpetrators involved. Please let us know if you have any additional questions or concerns.

Sincerely,
Epsilon Data Management, LLC



Jeanette Fitzgerald
General Counsel

cc: The Honorable Fred Upton, Chairman
The Honorable Henry A. Waxman, Ranking Member